

Executive Registry
73-671

OGC Has Reviewed

6 February 1973

MEMORANDUM FOR: Director of Central Intelligence

SUBJECT: Protection of Classified Information

1. This memorandum is for your information.



STATOTHR

3. Like the head of any agency, you are also responsible for protecting Agency information which is classified in accordance with the terms of Executive Order 11652, which goes beyond the pure source-and-method problem. Here again the traditional statutes provide the only sanctions.

4. Experience has shown that existing law does not provide a very effective enforcement tool. In the event of prosecution, the two basic statutes require demonstration that the information involved relates to the national defense and security. This is a question for the jury and must be produced in open court. We, thereby, authenticate the very information we are trying to protect. These laws also require either proof of intent or reason to believe that the information will be used to harm the U. S. or aid a foreign power. Again this is a question for the jury and is one in which proof is usually very difficult.

5. There are several provisions for specialized situations. Thus, the Atomic Energy Act makes the revelation of Restricted Data a crime but only if it is done with intent to injure the U. S. or secure an advantage from any foreign nation or with reason to believe that either of these will happen. Again, a statute defines Communications Intelligence as a category, and here all that is needed is to prove that it was knowingly and willfully transmitted to an unauthorized person. These two have never been fully tested in court. There is also a provision known as the Scarbeck statute, named after an individual who was prosecuted thereunder. This makes the knowing revelation of classified information a crime but applies only to Government employees who transmit such classified information to an agent of a foreign power. The opinion in the Scarbeck case provides that the prosecution must only prove that the material was classified. The court further held that whether the material was properly classified was not an issue to be considered by the court. For some years we have been advocating an amendment to the Scarbeck statute which would make it apply to any employee or former employee who gave classified information to an unauthorized person. This, we believe, would be quite an effective tool, but our best judgment has been that this Agency should not get out in front in seeking such authority.

6. A couple of years ago a Commission was set up to study a complete revision of the Federal Criminal Code, and we started to work with it in the areas pertaining to the protection of information. The Commission's work, including some of our suggestions, went to a Department of Justice Task Unit (established by direction of the President), with which we have been working for the past year. Its draft legislation, which was sent to OMB, was an improvement but still fell short of what we felt was needed. On 1 February we sent Mr. Rommel a letter accompanied by our suggested changes to the Department of Justice's draft. The Department of Defense independently made almost the same recommendations. I attach our comments and the sections of law which are under consideration. A new point is contained in section 1126 which provides for injunction to restrain violations. This is similar to the injunction authority in the Atomic Energy Act, but this as you may know has never been properly tested in the courts. However, if this proposed legislation passed in the form we recommend, it would be of very material assistance to the enforcement of the Director's responsibility for protection of information.

7. Separate from this general legislation, we are drafting legislation which would identify a category of "Intelligence Data" somewhat similar to the categories of Communications Intelligence and Restricted Data. Again we are without the guidance of court precedents, but we feel it could be another useful tool. This would be by an amendment to the National Security Act, which would place the bill with the two Armed Services Committees.

8. The general legislation will probably be introduced this spring but may become the subject of protracted debate. Our own provision concerning "Intelligence Data" will have to be discussed with our Subcommittees. It may be preferable to combine it with the general legislation which will be before the Judiciary Committees.

STATINTL



LAWRENCE R. HOUSTON
General Counsel

Attachment

cc: Executive Director
OLC
D/Security

1 FEB 1973

Mr. Wilfred H. Rommel
Assistant Director for
Legislative Reference
Office of Management and Budget
Washington, D. C. 20503

Dear Mr. Rommel:

This is in reply to your request of 17 January 1973 for our views on the Department of Justice's draft revision of Title 18, United States Code.

Enclosed are specific recommendations for changes in Chapter 2 entitled "Federal Criminal Jurisdiction," and in Chapter 11 entitled "Offenses Involving National Security." We are not commenting on the other Chapters of the draft revision, believing that they are generally outside the purview of this Agency's interest.

This Agency has been working for many years on the issues dealt with in Chapter 11, first with the Brown Commission and later with the Justice Department Task Unit. The focus of our work in this connection has been on those problems which are of particular interest to this Agency and to the intelligence community in general. The Brown Commission adopted a number of our suggestions for improvement in the laws in this respect. Further suggestions were incorporated by the Task Unit in the instant draft revision.

We believe that enactment of Chapter 11 with the changes as we have suggested in the enclosure would constitute a most significant improvement in the laws protecting national security information. Consequently, we strongly recommend support of the provisions of Chapter 11 with the changes we have suggested.

Sincerely,



STATINTL

John M. Maury
Legislative Counsel

Enclosure

1 February 1973

Central Intelligence Agency Comments OnJustice Department Draft: Revision of Title 18, U. S. CodeSection 204, Extraterritorial Jurisdiction of the United States.

We believe this section is too limited in that it fails to provide jurisdiction in cases of serious offenses against the United States if these offenses are committed abroad. This is particularly true of offenses against the national security. While subsection (b) provides extraterritorial jurisdiction in cases of treason, espionage and sabotage, it does not completely cover such closely related offenses as disclosing and mishandling of national security information (sections 1122 and 1123) and disclosing or unlawfully obtaining classified information (sections 1124 and 1125). As a minimum we would want to see extraterritorial jurisdiction extended to offenses under sections 1122 to 1125 and think that it might be prudent to extend it to all offenses under Chapter 11.

Section 1121, Espionage. We question the need for subsection (b)(1)(B) and feel that the traditional distinction between wartime and peacetime offenses is sufficient for the distinction between Class A felonies and lesser offenses. We are also concerned with the language of this subsection which in some places is vague and probably would become more so with technological advances. Terms such as "major" weapons systems or "major" element of defense strategy or "large scale" enemy attack are incapable of precise definition and subject

to argumentative interpretation in the case of prosecution. We also feel that the listing of particular objects of espionage as being more needful of protection through a higher grading of the felony invites nitpicking and "favorite cause" additions in the legislative process. Furthermore, it is our view that the more serious nature of the information in its effect on the United States can more appropriately be considered in connection with the sentencing process in the courts if the individual has been found guilty. However, if this subsection is to remain, we think there is a serious deficiency in the failure to include intelligence sources and methods as being worthy of this greater protection.

Section 1126, Definitions.

a. The offenses under sections 1121, 1122 and 1123 relate to "National Security Information." We would prefer to see these offenses limited to classified national security information. Classified information is specifically defined by Executive Order or statute and is clearly recognizable as having been classified. We do not believe there has been a successful prosecution for an offense involving national security information which was not classified information. We feel that the possibility of the need for prosecution of an offense involving unclassified national security information is too remote, and the difficulties of prosecution too great.

b. We think the attempted definition of "information relating to the national security" in section 1126(b)(8) is questionable and subject to severe criticism, particularly in its attempt to cover information, whether or not classified, which has not been officially disclosed to the public. This definition may be interpreted as an attempt to create an "Official Secrets Act" and will provide ammunition for critics of the proposed legislation who certainly will argue that it is a potential infringement on freedom of the press and freedom of information in general. Limiting offenses to those involving classified national security information would remove this difficulty in definition.

c. In addition, we think that the mere fact of nondisclosure of information in an official manner whether by Congress or by a public servant is much too broad since there is a great deal of material which is unclassified but which has simply not gone through the process of being officially disclosed.

d. Consequently, we would recommend that section 1126(b)(8) read as follows:

"Information relating to the national security"
means classified information which relates to the

national defense or to the conduct of foreign relations, including:"

e. It is to be noted that we also have deleted the words "involving the national defense" in the Department of Justice draft after the words "conduct of foreign relations." There can be many foreign relations matters which require the protection of classification and the laws which would not necessarily involve the national defense.

34. Extraterritorial Jurisdiction the United States.

Except as otherwise expressly provided by statute or treaty, the circumstances under which the United States has extraterritorial jurisdiction over an offense described in this title include the following:

- (a) the offense is a crime of violence and the victim or intended victim is a United States official;
- (b) the offense is treason, espionage, or sabotage against the United States;
- (c) the offense consists of a forgery or counterfeiting; uttering of forged copies or counterfeits; issuing without authority, seals, currency, instruments of credit, stamps, passports, or public documents issued by the United States; perjury or a false statement in an official proceeding of the United States; a false statement in a matter within the jurisdiction of the government of the United States; bribery or graft involving a public servant of the United States; or other fraud against the United States, or theft of property in which the United States has an interest; or, if committed by a national or resident of the United States, any other obstruction of or interference with a United States government function;
- (d) the offense is committed in whole or in part within the United States and the accused participates outside the United States, or the offense constitutes an attempt, conspiracy, or solicitation to commit an offense within the United States;
- (e) the offense involves entry of persons or property into the United States;
- (f) the offense is committed by a federal public servant who is outside the territory of the United States because of his official duties or by a member of his household residing abroad or by a person accompanying the military forces of the United States;

1/10/73

21. Espionage.

(a) Offense. A person is guilty of an offense, if, with intent, that information relating to the national security be used, or with knowledge that it may be used, to the prejudice of the safety or interest of the United States, or to the advantage of a foreign power, he knowingly:

- (1) communicates such information to a foreign power;
- (2) obtains or collects such information for a foreign power or with knowledge that it may be communicated to a foreign power; or
- (3) enters a restricted area with intent to obtain or collect such information for a foreign power or with knowledge that it may be communicated to a foreign power.

(b) Grading. An offense under this section is:

(1) a Class A felony:

(A) if committed during wartime or during a period of national defense emergency declared by the President or the Congress; or

(B) if the information directly concerns nuclear weaponry; military space vessels or satellites; early warning systems or other means of defense or retaliation against large scale enemy attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy;

(2) a Class B felony in any other case.

122. Disclosing National Security Information.

- (a) Offense. A person is guilty of an offense if he knowingly communicates information relating to the national security to a person not authorized to receive it.
- (b) Grading. An offense under this section is:
 - (1) a Class C felony if committed during wartime or during a period of national defense emergency declared by the President or the Congress; or
 - (2) a Class D felony in any other case.

1/10/73

3. Mishandling National Security Information.

(a) Offense. A person is guilty of an offense if:

- (1) being in possession or control of information relating to the national security, he recklessly permits its loss, destruction, theft, or communication to a person not authorized to receive it;
- (2) being in authorized possession or control of information relating to the national security:
 - (A) he intentionally fails to deliver it on demand to a public servant of the United States authorized to demand it;
 - (B) he knowingly fails to report promptly, to the agency authorizing him to possess or control such information, its loss, destruction, theft, or communication to a person not authorized to receive it; or
 - (C) he recklessly violates a duty imposed upon him by a statute or executive order, or by a regulation or a rule of the agency authorizing him to possess or control such information, which statute, order, regulation, or rule is designed to safeguard such information; or
- (3) being in possession or control of information relating to the national security which he is not authorized to possess or retain, he knowingly fails to deliver it promptly to a public servant of the United States entitled to receive it.

(b) Grading. An offense under this section is:

- (1) a Class E felony under the circumstances set forth in subsection (a)(2)(C);
- (2) a Class D felony in any other case.

1/10/73

4. Disclosing Classified Information.

Approved For Release 2002/05/17 : CIA-RDP75-00793R000100270010-9

- (a) Offense. A person is guilty of an offense if, being or having been in authorized possession or control of classified information, or having obtained such information as a result of his being or having been a public servant, he knowingly communicates such information to a person not authorized to receive it.
- (b) Exceptions to Liability as an Accomplice or Conspirator. A person not authorized to receive classified information is not subject to prosecution as an accomplice within the meaning of section 401 for an offense under this section, and is not subject to prosecution for conspiracy to commit an offense under this section.
- (c) Defense. It is a defense to a prosecution under this section that the information was communicated only to a regularly constituted committee of the Senate or the House of Representatives of the United States, or a joint committee thereof, pursuant to lawful demand.
- (d) Defense Precluded. It is not a defense to a prosecution under this section that the classified information was improperly classified.
- (e) Grading. An offense under this section is:
 - (1) a Class D felony if the person to whom the information is communicated is an agent of a foreign power;
 - (2) a Class E felony in any other case.

1/10/73

25. Unlawfully Obtaining Classified Information.

- (a) Offense. A person is guilty of an offense if, being an agent of a foreign power, he knowingly obtains or collects classified information which, in fact, he is not authorized to receive.
- (b) Defense Precluded. It is not a defense to a prosecution under this section that the classified information was improperly classified.
- (c) Grading. An offense under this section is a Class D felony.

126. General Provisions for Sections 1121 through 1125.

Approved For Release 2002/05/17 : CIA-RDP75-00793R000100270010-9

- (a) Injunctions to Restrain Violations. Upon evidence satisfactory to the Attorney General that any person is engaged, or about to be engaged, in any act or practice which constitutes or could constitute a violation of section 1121, 1122, 1123, 1124 or 1125, the Attorney General may bring an action in any district court of the United States to enjoin such act or practice, and, upon a proper showing, a permanent or temporary injunction or restraining order shall be granted by the court together with such other equitable relief as may be appropriate. Any action under this subsection shall be given precedence on the docket over all other causes, shall be heard at the earliest practicable date, and shall otherwise be expedited. Any appeal from the grant or denial of a permanent or temporary injunction or restraining order under this section shall be disposed of as soon as possible, but under any circumstances not later than 30 days from the filing of such appeal.
- (b) Definitions. As used in sections 1121 through 1125:
- (1) "agent" includes, in the case of a nation, a citizen or subject thereof;
 - (2) "authorized," when used in relation to the receipt, possession, or control of classified information or information relating to the national security, means with authority to have access to, to receive, to possess, or to control such information as a result of the provisions of a statute or executive order, or a regulation or rule thereunder, or as a result of position as a public servant;
 - (3) "classified information" means any information, regardless of its origin, which is marked or designated pursuant to the provisions of a statute or executive order, or a regulation or rule thereunder, as information requiring a specific degree of protection against unauthorized disclosure for reasons of national security;
 - (4) "communicate" means to impart information, to transfer information, or otherwise to make information available by any means, to a person or to the general public;
 - (5) "communications intelligence information" means information:
 - (A) regarding any procedures and methods used by the United States or any foreign power in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

1/10/73

Approved For Release 2002/05/17 : CIA-RDP75-00793R000100270010-9

- (B) regarding the use, design, construction, maintenance, or repair of any device or apparatus used, or prepared or planned for use, by the United States or any foreign power in the interception of communications and the obtaining of information from such communications by other than the intended recipients; or
 - (C) obtained by use of the procedures or methods described in paragraph (5)(A), or by a device or apparatus described in paragraph (5)(B);
- (6) "cryptographic information" means information:
- (A) regarding the nature, preparation, use or interpretation of any code, cipher, cryptographic system, or any other method of any nature used for the purpose of disguising or concealing the contents or significance or means of communications, whether of the United States or a foreign power;
 - (B) regarding the use, design, construction, maintenance, or repair of any device or apparatus used, or prepared or planned for use, for cryptographic purposes, by the United States or by a foreign power; or
 - (C) obtained by interpreting an original communication by the United States or by a foreign power which was in the form of a code or cipher or which was transmitted by means of a cryptographic system or any other method of any nature used for the purpose of disguising or concealing the contents or significance or means of communications;
- (7) "information" includes any property from which information may be obtained;
- (8) "information relating to the national security" means information, regardless of its origin, which has not been officially disclosed to the public by authority of Congress or by the lawful act of a public servant, and which relates to the national defense or to the conduct of foreign relations involving the national defense, including:
- (A) the military capability of the United States or of a nation at war with a nation with which the United States is at war;
 - (B) military planning or operations of the United States;

- (C) military communications of the United States;
 - (D) military installations of the United States;
 - (E) military weaponry, weapons development, or weapons research of the United States;
 - (F) restricted data as defined in section 11 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2014);
 - (G) intelligence of the United States, and information relating to intelligence operations, activities, plans, estimates, analyses, sources, and methods, of the United States;
 - (H) communications intelligence information or cryptographic information as defined in subsection (b)(5) or (b)(6); or
 - (I) in time of war, any other matter involving the security of the United States which might be useful to the enemy;
- (9) "restricted area" means any area of land, water, air, or space, which includes any facility of the United States, or of a contractor or subcontractor with or for the United States, to which access is restricted pursuant to a statute or executive order, or a regulation or rule thereunder, for reasons of national security.

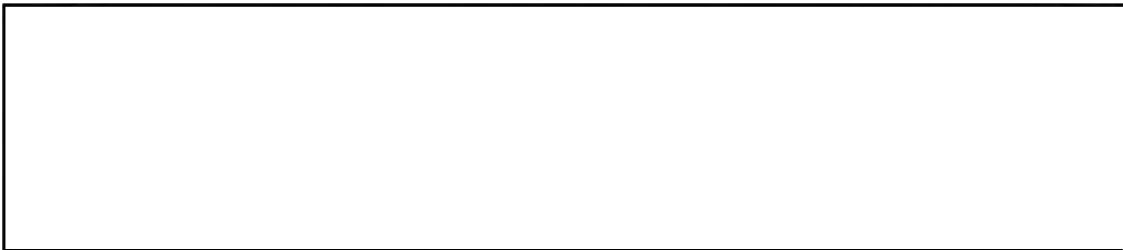
1/10/73

6 February 1973

MEMORANDUM FOR: Director of Central Intelligence

SUBJECT: Protection of Classified Information

1. This memorandum is for your information.



STATOTHR

3. Like the head of any agency, you are also responsible for protecting Agency information which is classified in accordance with the terms of Executive Order 11652, which goes beyond the pure source-and-method problem. Here again the traditional statutes provide the only sanctions.

4. Experience has shown that existing law does not provide a very effective enforcement tool. In the event of prosecution, the two basic statutes require demonstration that the information involved relates to the national defense and security. This is a question for the jury and must be produced in open court. We, thereby, authenticate the very information we are trying to protect. These laws also require either proof of intent or reason to believe that the information will be used to harm the U. S. or aid a foreign power. Again this is a question for the jury and is one in which proof is usually very difficult.

5. There are several provisions for specialized situations. Thus, the Atomic Energy Act makes the revelation of Restricted Data a crime but only if it is done with intent to injure the U. S. or secure an advantage from any foreign nation or with reason to believe that either of these will happen. Again, a statute defines Communications Intelligence as a category, and here all that is needed is to prove that it was knowingly and willfully transmitted to an unauthorized person. These two have never been fully tested in court. There is also a provision known as the Scarbeck statute, named after an individual who was prosecuted thereunder. This makes the knowing revelation of classified information a crime but applies only to Government employees who transmit such classified information to an agent of a foreign power. The opinion in the Scarbeck case provides that the prosecution must only prove that the material was classified. The court further held that whether the material was properly classified was not an issue to be considered by the court. For some years we have been advocating an amendment to the Scarbeck statute which would make it apply to any employee or former employee who gave classified information to an unauthorized person. This, we believe, would be quite an effective tool, but our best judgment has been that this Agency should not get out in front in seeking such authority.

6. A couple of years ago a Commission was set up to study a complete revision of the Federal Criminal Code, and we started to work with it in the areas pertaining to the protection of information. The Commission's work, including some of our suggestions, went to a Department of Justice Task Unit (established by direction of the President), with which we have been working for the past year. Its draft legislation, which was sent to OMB, was an improvement but still fell short of what we felt was needed. On 1 February we sent Mr. Rommel a letter accompanied by our suggested changes to the Department of Justice's draft. The Department of Defense independently made almost the same recommendations. I attach our comments and the sections of law which are under consideration. A new point is contained in section 1126 which provides for injunction to restrain violations. This is similar to the injunction authority in the Atomic Energy Act, but this as you may know has never been properly tested in the courts. However, if this proposed legislation passed in the form we recommend, it would be of very material assistance to the enforcement of the Director's responsibility for protection of information.

7. Separate from this general legislation, we are drafting legislation which would identify a category of "Intelligence Data" somewhat similar to the categories of Communications Intelligence and Restricted Data. Again we are without the guidance of court precedents, but we feel it could be another useful tool. This would be by an amendment to the National Security Act, which would place the bill with the two Armed Services Committees.

8. The general legislation will probably be introduced this spring but may become the subject of protracted debate. Our own provision concerning "Intelligence Data" will have to be discussed with our Subcommittees as it may be preferable to combine it with the general legislation which will be before the Judiciary Committees.

STATINTL

LAWRENCE R. HOUSTON
General Counsel

Attachment
OGC:LRH:jeb
cc: Executive Director
OLC
D/Security
OGC chrono
✓subject CIA Acts and Statutes

Note for File:

Attachment - 1 February 1973 letter from Legislative Counsel to OMB re Department of Justice's draft revision of Title 18

Excerpt from Morning Meeting Minutes
5 February 1973

In response to the Director's question, Maury, Thuermer, and the Executive Director highlighted our concerns and action taken to date with respect to an article New York Times correspondent Seymour Hersh is working on that is apt to expose sensitive intelligence operations. Houston noted that the DCI has a statutory responsibility to protect sources and methods, and efforts are under way to enhance enforcement by rewriting portions of the Criminal Code. Our suggested revisions to the Code are with OMB. The Director suggested that Brigadier General Scowcroft be briefed on this matter. (ACTION: General Counsel to prepare briefing paper)

SENDER WILL CHECK CLASSIFICATION TOP AND BOTTOM			
UNCLASSIFIED	CONFIDENTIAL	SECRET	
OFFICIAL ROUTING SLIP			
TO	NAME AND ADDRESS	DATE	INITIALS
1	Executive Director		
2	The Director		
3			
4			
5			
6			
ACTION	DIRECT REPLY	PREPARE REPLY	
APPROVAL	DISPATCH	RECOMMENDATION	
COMMENT	FILE	RETURN	
CONCURRENCE	INFORMATION	SIGNATURE	
Remarks: Attached is an attempt to describe in nontechnical language the current status of the law pertaining to protection of classified information.			
<div style="border: 1px solid black; width: 300px; height: 50px; margin: 0 auto;"></div> <p>Lawrence R. Houston</p>			
FOLD HERE TO RETURN TO SENDER			
FROM: NAME, ADDRESS AND PHONE NO.			DATE
General Counsel			2/6/73
UNCLASSIFIED	CONFIDENTIAL	SECRET	

FORM NO. 1-67

237

Use previous editions

(40)

STATINTL

NOTE ATTACHED TO MEMORANDUM DATED 6 FEBRUARY 1973

Approved For Release 2002/05/17 : CIA-RDP75-00793R000100270010-9

EXECUTIVE SECRETARIAT

Routing Slip

TO:		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	S/MC				
4	DDS&T				
5	DDI				
6	DDM&S				
7	DDO				
8	D/DCI/IC				
9	D/DCI/NIO				
10	OGC	✓			
11	OLC				
12	IG				
13	Compt				
14	D/Pers				
15	D/S				
16	DTR				
17	Asst/DCI				
18	AO/DCI				
19					
20					
21					
22					

SUSPENSE

Date

Remarks:

*He will say when you hang
up phone to speak with
phone.*

Done



STATINTL

NOTE ATTACHED TO MEMORANDUM DATED 6 FEBRUARY 1973